(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－275114

(43)公開日　平成10年(1998)10月13日

| (51)Int.Cl.⁶ | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３１０ | Ｃ０６Ｆ | 12/14 | ３１０Ｋ |
| | 12/00 | ５３７ | | 12/00 | ５３７Ａ |
| | 15/00 | ３３０ | | 15/00 | ３３０Ｄ |

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）

(21)出願番号　特願平9－80909

(22)出願日　平成９年(1997)３月31日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　磯山　朋宏
岡山県岡山市磨屋町10番12号　株式会社富士通岡山システムエンジニアリング内

(72)発明者　波江　裕司
岡山県岡山市磨屋町10番12号　株式会社富士通岡山システムエンジニアリング内

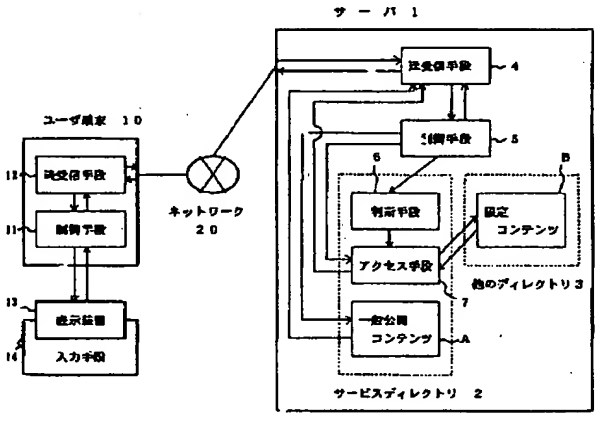
(74)代理人　弁理士　福井　豊明

(54)【発明の名称】　インターネットのコンテンツセキュリティ方法およびシステム

(57)【要約】

【課題】　インターネットのシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。

【解決手段】　ユーザが自由に閲覧することができるサーバ上のサービスディレクトリ以外の他のディレクトリに特定用途の限定コンテンツを設け、ユーザ端末より特定のパラメータを与えることによって、上記限定コンテンツへのアクセス許可が与えられた場合に上記限定コンテンツをアクセスする。よって、上記限定コンテンツへのアクセス許可が与えられた者だけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていない者が該限定コンテンツへアクセスすることを確実に防止することのできる。



【特許請求の範囲】
【請求項１】　ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、
上記限定コンテンツを上記サーバ上のサービスディレクトリ以外の他のディレクトリに設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツをアクセスすることを特徴とするインターネットのコンテンツセキュリティ方法。
【請求項２】　ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティシステムにおいて、
上記サーバ上のサービスディレクトリ以外の他のディレクトリに備えた上記限定コンテンツと、
上記サーバ上のサービスディレクトリに設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段とを備えたことを特徴とするインターネットのコンテンツセキュリティシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明はインターネットシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。
【０００２】
【従来技術】現在、世界中にはりめぐらされたネットワークを介して接続された不特定多数のユーザがサーバ上に作成されたコンテンツを自由に閲覧することができるインターネットシステムが普及し、その中で特定のユーザだけを対象としたサービスも増加している。このサービスは、ユーザＩＤ、パスワード等を管理し、パスワードチェックでアクセスの許可が与えられた特定のユーザであると判断された場合に、特定のユーザを対象にして作成された限定コンテンツを閲覧することができるようにしている。以下、この従来のセキュリティシステムについて図４に基づいて説明する。
【０００３】インターネットシステムにおいて利用されるサーバ３１上には閲覧ソフトであるブラウザによってユーザ端末３３からネットワーク３４を介して自由に閲覧することができるサービスディレクトリ３２が設けられており、該サービスディレクトリ３２に一般公開される一般公開コンテンツＡおよび上記限定コンテンツＢ等が編集されている。
【０００４】上記ユーザ端末３３より一般公開コンテンツＡのＨＴＭＬページを閲覧する場合、上記ブラウザより目的とするＨＴＭＬページのサーバアドレスおよびサーバ内アドレスであるＵＲＬを直接入力するか、または現在閲覧中のＨＴＭＬページ内に設けられたリンクを選択し実行することによってアクセスし閲覧することができる。
【０００５】また、上記ユーザ端末３３より上記限定コンテンツＢのＨＴＭＬページを閲覧する場合、上記一般公開コンテンツＡの場合と同様にしてユーザＩＤおよびパスワード等の入力を行うＨＴＭＬページ（以下、パスワードページと言う）を表示させる。次に該パスワードページよりユーザＩＤおよびパスワードを入力すると、サーバ上に予め備えられたデータベースのデータに基づいて、上記のように入力されたユーザＩＤは存在するか、またパスワードが正しいか等のチェックが行われ、上記限定コンテンツＢへのアクセス許可が与えられたユーザであると判断された場合に該限定コンテンツＢにアクセスし閲覧することができる。
【０００６】しかしながら、一般にサーバ３１上の上記サービスディレクトリ３２に編集されたコンテンツは一般公開コンテンツＡ、限定コンテンツＢ等の区別に関係なく、上記ブラウザ上でこれらコンテンツのＵＲＬを直接入力することでアクセスすることができる。したがって、上記のような従来のセキュリティでは、上記パスワードページは一般公開コンテンツＡ等にリンクを設けるか、または直接ＵＲＬを公開するなどしているのに対して、限定コンテンツＢはそれ自体のＵＲＬを非公開とすることによって、上記パスワードページを経ないで上記限定コンテンツＢにアクセスされることを防止している。
【０００７】
【発明が解決しようとする課題】上記のような従来のセキュリティでは、もし上記限定コンテンツＢの場所すなわちＵＲＬが知られれば、アクセス許可が与えられていないユーザであっても、上記ブラウザ上で該ＵＲＬを直接入力することで、上記限定コンテンツＢへのアクセスを行うことができることになる。
【０００８】よって上記限定コンテンツＢのＵＲＬは非公開とされているが、例えば一般公開および限定コンテンツＢのＵＲＬが似かよっている場合に、アクセス許可が与えられていないユーザが一般公開コンテンツＡのＵＲＬより上記限定コンテンツＢのＵＲＬを類推して入力したり、また偶然に上記限定コンテンツＢのＵＲＬを入力したりして上記限定コンテンツＢのＵＲＬが知られてしまうことや、以前アクセス許可を有していたユーザが資格を喪失した後に、以前に知り得た上記限定コンテンツＢのＵＲＬを利用することが起こりえる。
【０００９】以上のように従来のセキュリティでは、ア

クセス許可が与えられていないユーザによって上記限定コンテンツＢへアクセスされることを完全に防止することができなかった。

【００１０】本発明は上記の事情に鑑みて提案されたものであり、上記限定コンテンツへのアクセス許可が与えられたユーザだけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていないユーザが該限定コンテンツへアクセスすることを確実に防止することのできるインターネットのコンテンツセキュリティ方法およびシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は上記目的を達成するために以下の手段を採用している。すなわち、ユーザが自由に閲覧することができるサービスディレクトリ２をサーバ１上に設け、ユーザ端末１０より特定のパラメータを与えることによって、上記サービスディレクトリ２に設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツＢへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、上記限定コンテンツＢを上記サーバ１上のサービスディレクトリ２以外の他のディレクトリ３に設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツＢをアクセスするという手段を採用している。

【００１２】具体的には、上記サーバ１上のサービスディレクトリ２以外の他のディレクトリ３に備えた上記限定コンテンツＢと、上記サーバ１上のサービスディレクトリ２に設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツＢをアクセスするアクセス手段とを備えることによって実現する。

【００１３】

【実施の形態】図１は本発明のインターネットのコンテンツセキュリティシステムの適用されるネットワークの概念図であり、図２は本発明のインターネットのコンテンツセキュリティシステムの一実施例のブロック図であり、図３は上記システムにおける処理手順を示すフロー図であり、以下図に基づいて説明する。

【００１４】本実施例において、サーバ１上のサービスディレクトリ２にはパスワードページを含む一般公開コンテンツＡ、パラメータ判断手段６、アクセス手段７を、サービスディレクトリ２以外の他のディレクトリ３には限定コンテンツＢを設けている。

【００１５】ユーザ端末１０よりネットワーク２０を介して接続されたサーバ１上の上記限定コンテンツＢを閲覧する場合、まず最初に上記サービスディレクトリ２に設けた上記パスワードページを表示させる。この手順は、上記ユーザ端末１０のキーボードやマウス等の入力手段１４で上記ユーザ端末の制御手段１１により起動されたブラウザ上から直接上記パスワードページのＵＲＬを入力するか、または一般公開コンテンツＡのＨＴＭＬページ内に設けられた上記パスワードページのリンクを選択して実行（Ｓ１）すれば、上記パスワードページのＵＲＬがユーザ端末１０の送受信手段１２から、該ＵＲＬ中のサーバアドレスに基づいてネットワーク２０を介して上記サーバ１の送受信手段４へ、次に該送受信手段４より制御手段５へ送られる（Ｓ２）。該制御手段５は送られたＵＲＬ中のサーバ内アドレスに基づいて上記パスワードページを上記送受信手段４、ネットワーク２０を介して上記ユーザ端末１０の上記送受信手段１２へ送る。次に上記ユーザ端末１０では、送信されてきた上記パスワードページが上記ブラウザによって上記ユーザ端末１０の表示装置１３に表示される（Ｓ３）。

【００１６】そして次に、該パスワードページにユーザが上記入力手段１４によってパラメータとしてユーザＩＤおよびパスワードを与えて入力（Ｓ４）すれば、上記パスワードページのＵＲＬと同様にして上記送受信手段１２から上記ネットワーク２０、上記サーバ１の送受信手段４を介して上記制御手段５へ送信され、該制御手段５によりパラメータ判断手段６が起動される。該パラメータ判断手段６では、サーバ１上の上記サービスディレクトリ２以外の他のディレクトリ３に設けられたデータベースに予め蓄積されたデータに基づいてユーザ端末１０より送信されてきた上記ユーザＩＤが存在するか、また上記パスワードが正しいのかのチェック（Ｓ５）を行っている。

【００１７】その結果、上記限定コンテンツＢへのアクセス許可が与えられたユーザであると判断した場合、アクセス手段７が上記パラメータに対応して予め設定された限定コンテンツＢの初期ＨＴＭＬページ（例えば図４に示すメニューページ等）へアクセス（Ｓ６）を行い、該初期ＨＴＭＬページを上記パスワードページと同様にして上記ユーザ端末１０へ送信し、上記表示装置１３に表示（Ｓ７）させる。この初期ＨＴＭＬページには少なくとも１つの次表示項目２１（例えば図４に示すメニューページでは次に表示することのできるＨＴＭＬページの項目等）が掲げられており、ユーザが該次表示項目２１のいずれかを指示することによって、次画面を選択することができるようになっている。すなわち、上記次表示項目２１にはそれぞれに該次表示項目の格納場所のディレクトリを記載したフルパスの表示ＨＴＭＬ名２２がユーザには見えない形式（画面には表示されず上記ユーザ端末１０のメモリ等に格納される）で隠しパラメータとして付与されており、また該フルパスの表示ＨＴＭＬ名２２に追加して上記アクセス手段７を起動する旨の指定がなされている。これによって、上記のようにユーザの指示に基づいて選択された特定の次表示項目２１に対応した次画面を表示することができる。

【００１８】尚、上記チェックの結果、上記限定コンテンツＢへのアクセス許可が与えられたユーザでないと判

断した場合、上記初期ＨＴＭＬページへのアクセスは行われず、アクセス許可がない旨の表示が上記表示装置１３になされる（Ｓ８）。

【００１９】次に、ユーザが選択した上記次表示項目２１を実行（Ｓ９）すれば、該次表示項目２１のフルパスの表示ＨＴＭＬ名２２がパラメータとして上記パスワードページのＵＲＬと同様にして上記制御手段５に送信され上記アクセス手段７が起動される。該アクセス手段７では送信されたパラメータであるフルパスの表示ＨＴＭＬ名２２によって選択された次表示をアクセス（Ｓ１０）して、該次表示が上記パスワードページと同様にしてユーザ端末１０へ送信され、上記表示装置１３に表示（Ｓ１１）される。これ以降の限定コンテンツＢの次表示へのアクセスは、上記次表示へのアクセス手順と同様にして行われる。

【００２０】また、上記限定コンテンツＢを利用中のユーザは、どの時点であっても閲覧中の画面に設けられたリンクを上記入力手段１４で選択して実行するか、または上記ブラウザ上から直接一般公開コンテンツＡのＵＲＬを上記入力手段１４で入力することによって、上記限定コンテンツＢの閲覧を終了して一般公開コンテンツＡの閲覧に移ることができる。

【００２１】

【発明の効果】本発明のインターネットのコンテンツセキュリティ方法およびシステムによれば、限定コンテンツをサーバ上のサービスディレクトリ以外の他のディレクトリに設け、アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段を上記サーバ上のサービスディレクトリに設けたことにより、該限定コンテンツへのアクセス許可が与えられていないユーザからのアクセスを確実に防止することができる。

【図面の簡単な説明】

【図１】本発明の適用されるネットワークの概念図である。

【図２】本発明の一実施例のブロック図である。

【図３】本発明の一実施例のフロー図である。

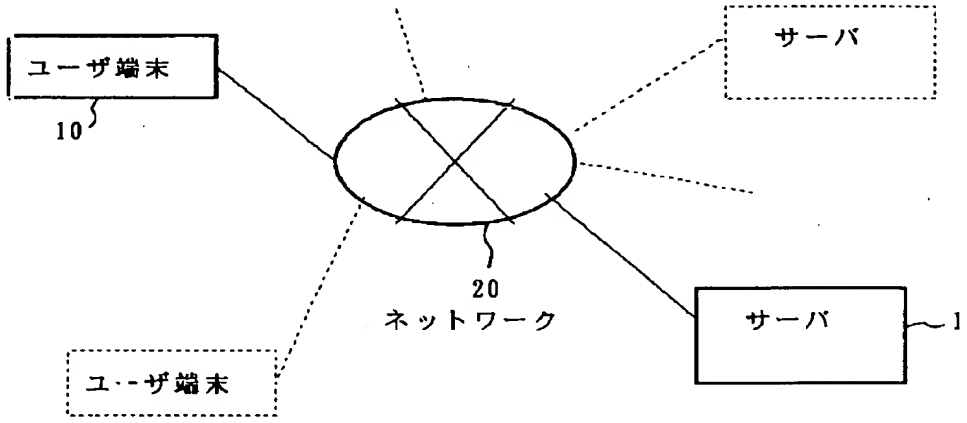
【図４】本発明の一実施例の画面例である。

【図５】従来のシステム概念図である。

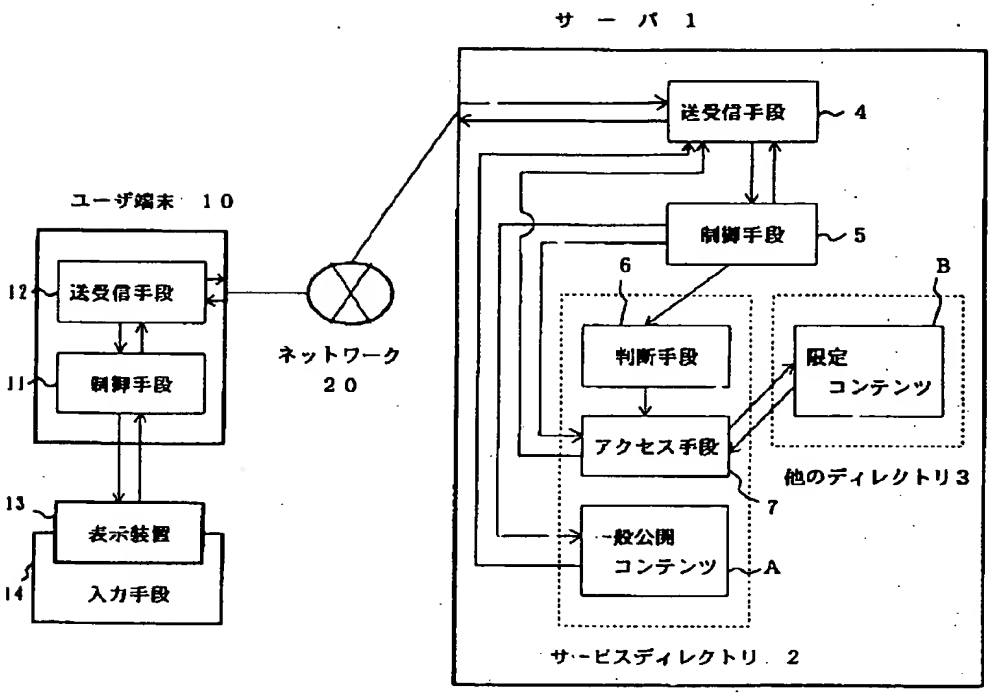
【符号の説明】

| | |
|---|---|
| １、３１ | サーバ |
| ２　３２ | サービスディレクトリ |
| ３ | 他のディレクトリ |
| ４、１２ | 送受信手段 |
| ５、１１ | 制御手段 |
| ６ | パラメータ判断手段 |
| ７ | アクセス手段 |
| １０、３３ | ユーザ端末 |
| １３ | 表示装置 |
| ２０、３４ | ネットワーク |
| Ａ | 一般公開コンテンツ |
| Ｂ | 限定コンテンツ |

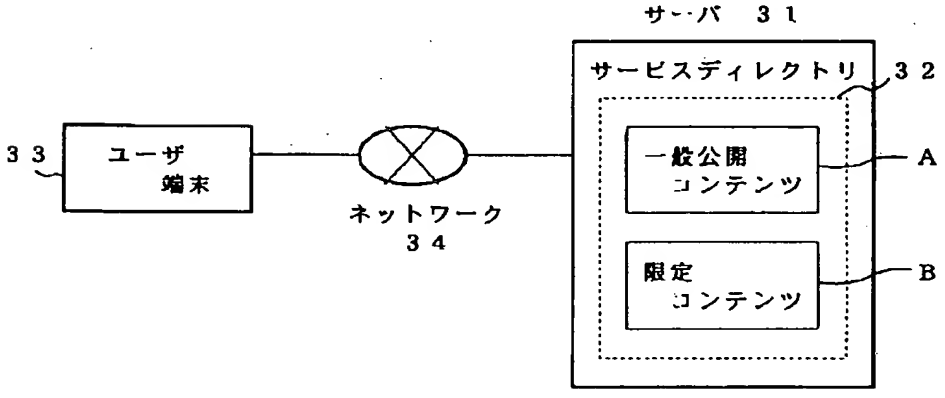
【図１】



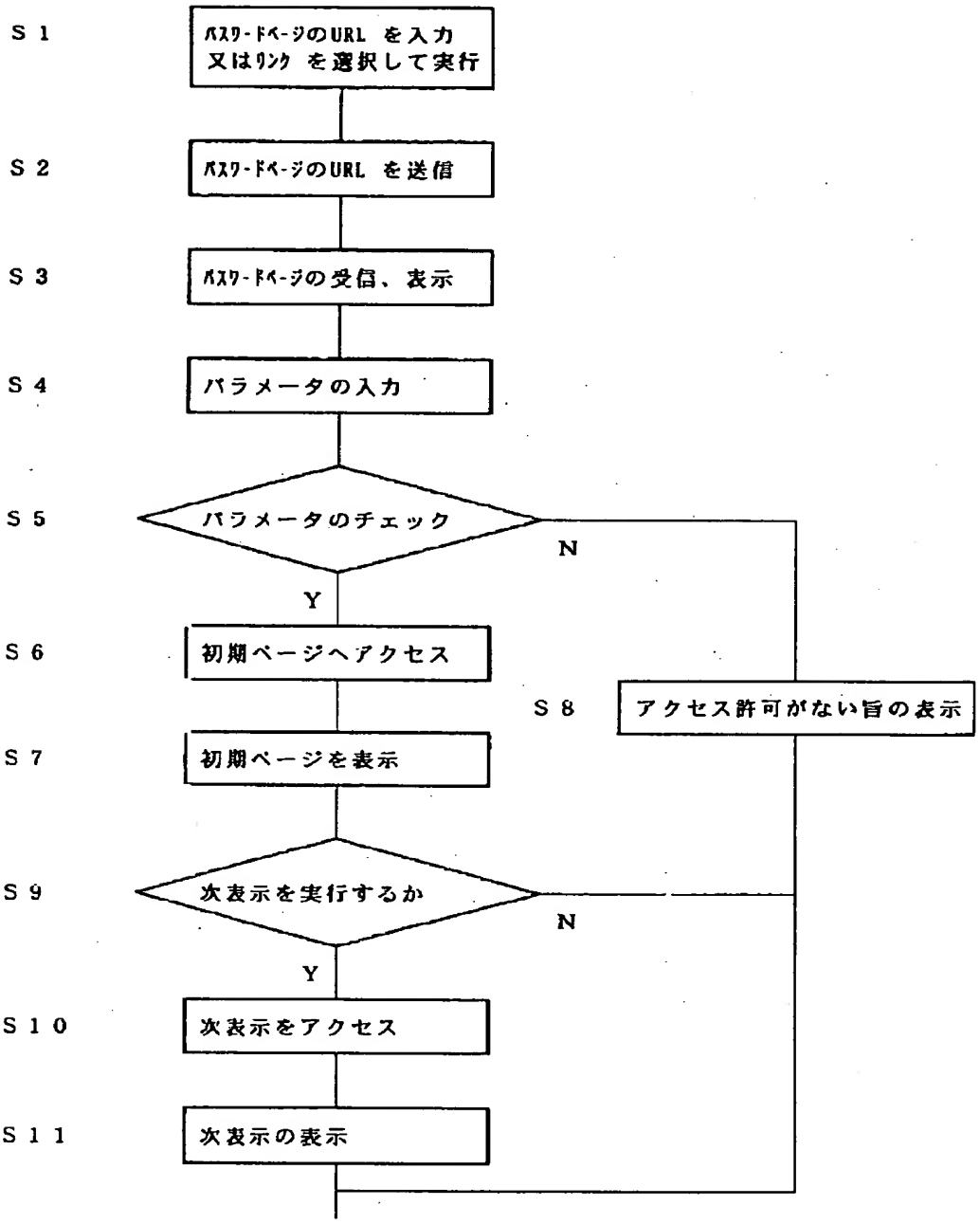
【図2】




【図5】



【図3】



【図4】